Comment Report

STATEWIDE POLICY: ESSENTIAL INFORMATION SECURITY ROLES

FEBRUARY 11, 2009

Scope

This report contains the comments and responses for the statewide review of the *Statewide Policy: Essential Information Security Roles*, which was available for review January 8th to 30th, 2009.

Executive Summary

The purpose of this report is to:

1. Publish received comments,
2. indicate status of proposed changes, and
3. respond to each comment.

Comments were received from five agencies, over the period of January 21st through February 3rd. Some initial comments were re-submitted after further refinement. The initial comments were set aside and the final comments appear herein. The comments and feedback appear to emanate from the technical audience, and their comments were in the following areas:

1. Proposed prose changes in the requirements. These have largely been rejected because the changes would materially alter the requirements. They are addressed herein.
2. Questions regarding supporting services from ITSD. These are service issues, not statewide policy issues, and have not been included herein. The service issues have been referred to ITSD for disposition.
3. Comments regarding details of referenced documents. These have been addressed herein.

The respondents did not appear to include agency policy-makers - those individuals nominally responsible for implementing policy (i.e., directors, administrators, etc.); and *policy-level* concerns were not detected within the

comments. The upshot being that we are aware of no policy-maker issues stemming from this policy.

The recommendation from the policy manager to the State of Montana Chief Information Officer is to approve the policy based on the response herein.

Comments/Feedback with Response

Item	Comment/Suggestion	Response/ Disposition	Status
1.	**COMMENT:** Statewide Policy: Essential Information Security Roles **Section I Purpose** The title says Essential Information Security Roles yet the purpose is to implement an entire program. We think either the title has to change or the purpose does. If one of your goals is to get the entire security program going in each agency -- biting it off into realistic chunks is a better approach. Getting each agency to think through who would perform the duties defined for the various roles and establishing that within their own agencies is a very good place to start. Our commentary will be based on that 'bite-sized' approach. Given that… we suggest that the purpose be changed to something more like (see items in blue).... This Essential Information Security Roles Policy (Policy) establishes the ~~requirements~~ roles and responsibilities needed to implement a computer security program based upon National Institute of Standards and Technology (NIST) guidance, specifically using the NIST risk management framework.	**RESPONSE:** The proposed change is rejected because it materially changes the requirement. §2-15-114 MCA requires that agencies implement a program. §2-17-534 MCA provides the means to accomplish security policy in a consistent, common manner; across agencies. This policy (and the planned NIST-based information security policies and standards) establishes the common “how” at the *policy-maker* level, thereby providing the vehicle to implement these two statutes together.	No Change

Item	Comment/Suggestion	Response/ Disposition	Status
2.	**COMMENT:** Statewide Policy: Essential Information Security Roles **Section II Policy Statement** Referencing the entire document (NIST800-100) without specifying what sections are directly related to this *Roles* policy is a bit of a disservice to the folks you are asking to review as well as implement this *roles* policy. Our suggestion is for you to reference the appropriate sections. We suggest Chapter 2 section 2.3 "Key Governance Roles and Responsibilities", Chapter 8 section 8.2 "Security Planning Roles and Responsibilities", and perhaps Chapter 11 Section 11.1 "Certification, Accreditation, and Security Assessments Roles and Responsibilities".	**RESPONSE:** All sections of NIST SP800-100 are applicable to the understanding of a NIST-based information security program; and the inherent roles. The agency is encouraged to leverage the content of this and other NIST publications as necessary to understanding and implementing a NIST-based security program. Under the FISMA/NIST framework, the agency is free to reference specific NIST prose within their own (local) version of a policy or standard, to include adding prose beyond (but not negating) the statewide standard requirements.	No Change
3.	**COMMENT:** Statewide Policy: Essential Information Security Roles **Section VI Authorizations, Roles & Responsibilities** You reference only section II "Authorizations, Roles and Responsibilities" in the Statewide Guidelines for Implementation of Information System Security. And while that section does provide the authority for this new policy that you are seeking commentary on…. It also includes a section V referencing "Agency Staffing for IS Security Purposes". This is not in conflict with the new policy on roles but adds to the confusion. Why would this verbiage be included here? We don't believe that anything beyond the first paragraph as edited in blue below should be included in the secondary policy that you direct us to for authorization. The second paragraph is focused on one role	**RESPONSE:** The guidelines document only offers additional guidance; the policy contains the (mandatory) requirement.	No Change

Item	Comment/Suggestion	Response/ Disposition	Status
	only, whereas the policy you are seeking commentary on seems to assume there are multiple roles. That may avoid some of the confusion.		
4.	**COMMENT:** Statewide Policy: Essential Information Security Roles V. Agency Staffing for IS Security Purposes Each state agency will need to have competent staff assigned ~~for the following functions~~ in order to insure appropriate implementation and ongoing management of the IS security program. An agency will be authorized to assign staff in a manner consistent with its size, complexity and financial capabilities including that IS Security staff may be obtained through contracted IS service providers. ~~*Information Security Officer (ISO):* The ISO will have overall responsibility for ensuring the agency's compliance with the IS security program, policies and standards. The ISO will be the primary point of contact with DOA's Information Technology Services Division (ITSD); will ensure agency staff are appropriately educated regarding IS security policies, standards and practices; and will investigate and address actual and suspected IS security threats and violations within the agency.~~	**RESPONSE:** The change is rejected because it would materially alter the requirement.	No Change
5.	**COMMENT:** **Section VII Requirements**	**RESPONSE:** Under the FISMA/NIST framework, the agency is free to increase the	No Change

Item	Comment/Suggestion	Response/ Disposition	Status
	In this section you reference NIST SP800-30 but only paragraph 2.3 which highlights the key roles. We appreciate this more direct focus. The difficulty is that there is not quite enough clarification from you as to what these roles mean to us at the State of Montana, particularly at the highest level -- Senior Management. Is this cabinet level staff in the governor's office or is it to be represented by each Agency and would include the Director and their management team? A simple phrase extension in the requirements section should clarify this…. such as: Agencies shall use NIST Special Publications 800-30, paragraph 2.3 (NIST SP800-30) Risk Management Guide for Information Technology Systems as general guidelines in assigning roles and responsibilities within their own agencies, starting at the top of their organization hierarchy.	requirement within their own version of a policy or standard, to include adding local prose beyond (but not negating) the statewide standard requirements.	
6.	**COMMENT:** **Section VIII Compliance** Here you state that compliance is based on the implementation and use of risk management processes and procedures aligned with NIST guidance. While we may agree in principle with that goal, we believe that the policy is about defining the roles for one's own agency. In this regard, having something more achievable in the compliance section as well as insuring currency might be more apropos. We suggest something like…. Agency Information Security Officers (ISO) will	**RESPONSE:** The change is rejected because it would materially alter the requirement. Under the FISMA/NIST framework, the agency is free to alter the prose within their own version of a policy or standard, to include adding local requirements beyond (but not negating) the statewide standard requirements. Should the agency put the proposed level of detail into their local policy, it will be obsolete/out-of-compliance unless the named individual is in that role and organization.	No Change

Item	Comment/Suggestion	Response/ Disposition	Status
	provide to the ITSD Information Security Officer (currently Kevin Winegardner) their Agency Security Staffing Roles and Responsibilities document on an annual basis effective mm/dd/yyyy. This document will clearly identify the individuals assigned to the various roles and what their specific duties are in meeting the responsibilities as identified in this policy references.		